What is claimed is:

1. An unauthorized information detecting system, characterized in that the number of values of some field in the header of the packet transmitted through an internet circuit is monitored, and in case the number of values of the field reaches a predetermined number or a predetermined ratio within a predetermined time, it is judged that an unauthorized attack is performed.

2. The unauthorized information detecting system according to claim 1, characterized in that the number of values of said field and the number of packets are monitored.

3. The unauthorized information detecting system according to claim 1, characterized in that the number of values of said field and the number of communications (the number of octets/the number of bits) are monitored.

4. The unauthorized information detecting system according to claim 1 or 2, characterized in that the values of said field is configured by a combination of a plurality of fields.

5. The unauthorized information detecting system according to any of claims 1 to 4, characterized in that when the number of hops of said information on the internet circuit reaches a predetermined value or the number of hops carried by the packet corresponding to a specific field or a combination of fields changes, the relevant information is identified as unauthorized information.

6. An unauthorized information detecting system, characterized in that when the number of hops of said information on the internet circuit

reaches a predetermined value or the number of hops carried by the packet corresponding to a specific field or a combination of fields changes, the relevant information is identified as unauthorized information.

7. An unauthorized attack source searching system, characterized in that the number of values of some field in the header of the packet transmitted through an internet circuit is monitored, and in case the number of values of the field reaches a predetermined number or a predetermined ratio within a predetermined time, it is judged that an unauthorized attack is performed, and the number of values of the field is monitored at a plurality of places of the internet circuit, so that an unauthorized source is searched.

8. The unauthorized attack source searching system according to claim 7, characterized in that the values of said field are configured by an individual combination of plurality of fields within the header.

9. The unauthorized attack source searching system according to claim 8, characterized in that, when the number of hops of said information on the internet circuit reaches a predetermined value or the number of hops carried by the packet corresponding to a specific field or a combination of the fields changes, the relevant information is identified as unauthorized information.